PUBLIC KEY INFRASTRUCTURE (PKI)
&
COMMON ACCESS CARD

Private Key

ENCRYPTION
DIGITAL SIGNATURE
USER IDENTIFICATION
USER AUTHENTIFICATION
USER NONREPUDIATION
DATA INTEGRITY
DATA CONFIDENTIALITY

Public Key

Armed Forces of the United States

U.S. Marine Corps

Active Duty

Parker IV, Christopher J.

Pay Grade	Rank
E6	**SSGT**

Issue Date
2000SEP19
Expiration Date
2003SEP18

Geneva Conventions Identification Card
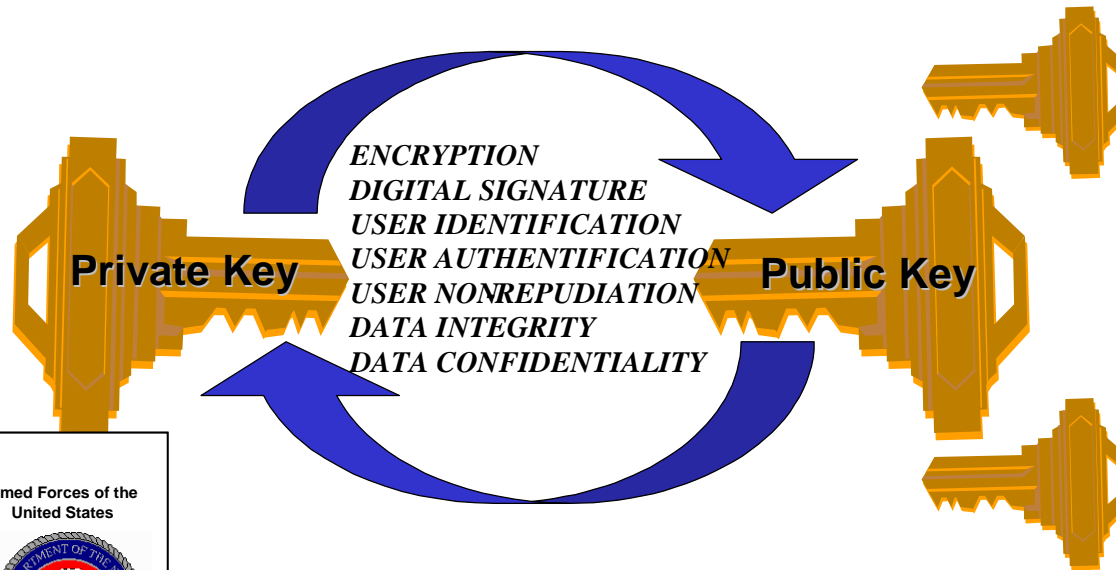
LtCol Beck (APM)
CAC, SCT, PKI, PK-E

Purpose

   The purpose of this presentation is to provide Regional Contractor Officers Representatives and Customer Technical Representatives an overview of USMC CAC and PKI activities in support of NMCI.
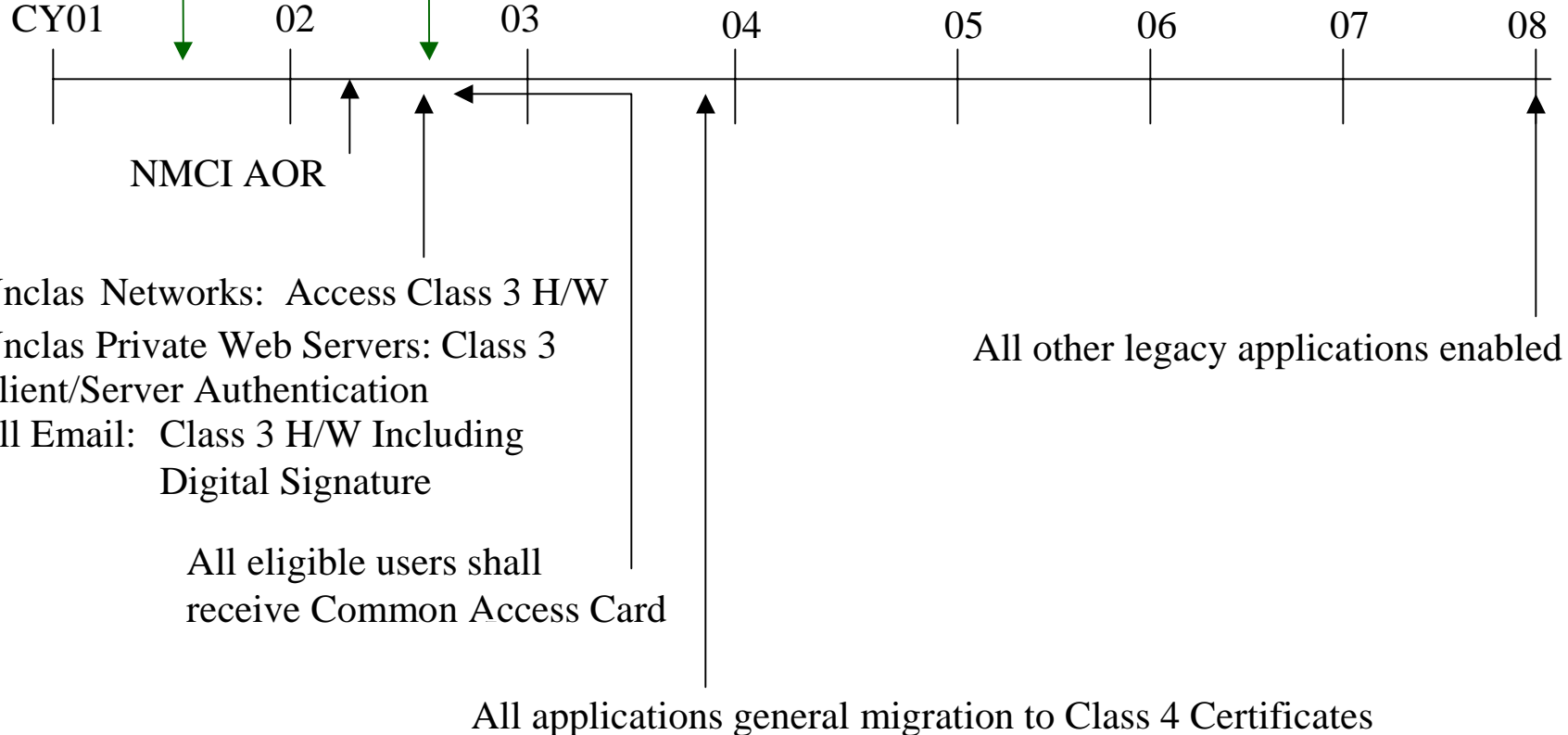
DEPSECDEF Memo 10 Nov 1999

- CAC shall be the standard ID card for active duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel
- CAC shall be primary store for user PKI keys and certificates
  - still requirement for PKI outside of CAC (e.g., SIPRNET)
- CAC shall be issued and maintained via DEERS/RAPIDS infrastructure
  - 1 year to update 1800 DoD DEERS/RAPIDS workstations
  - Normal replacement vice mass issuance

PK-E/PKI/CAC/NMCI

PKI Class 3 Registration Capability

(DEERS/RAPIDS & RA/LRA Infrastructure) FOC

All users issued Class 3 Certificates

CY01   02   03   04   05   06   07   08

NMCI AOR

- Unclas Networks: Access Class 3 H/W
- Unclas Private Web Servers: Class 3
  Client/Server Authentication
- All Email: Class 3 H/W Including
  Digital Signature

All other legacy applications enabled

All eligible users shall
receive Common Access Card

All applications general migration to Class 4 Certificates

CAC & PKI PROVIDE FOR:

Personnel Identification
Replaces the "ID" Card

Building Access

Systems & Network Access
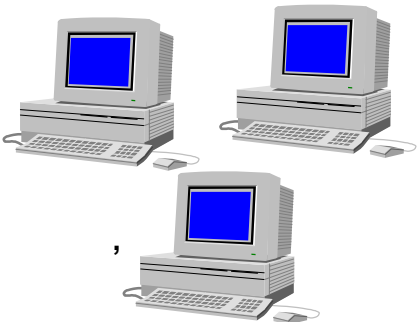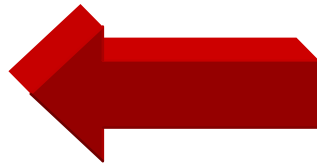
CAC & PKI Provide For: (cont.)

- Message Confidentiality

- Message Integrity

- Message Sender/Receiver Authentication

- Message Technical Non Repudiation

CAC/PKI Approach

- As NMCI users are activated they will be issued a CAC via DEERS/RAPIDS that will have three DoD PKI certificates (Identity and E-mail- Encryption, Signature)

- Current Marine Corps strategy is to issue software certificates through the DoD CA until CAC status has stabilized

Government PKI Role

- Operational Oversight - Federal, DoD, & DON Compliance/Requirements
- Configuration Management
    - Software
    - Test Bed
- RA Functions
    - Forward Revocation Request to CA
    - RRA/LRA Training
    - Test Bed
- PKI Technical Support Team
    - Audit
    - Technical Assistance
- Tactical Functions
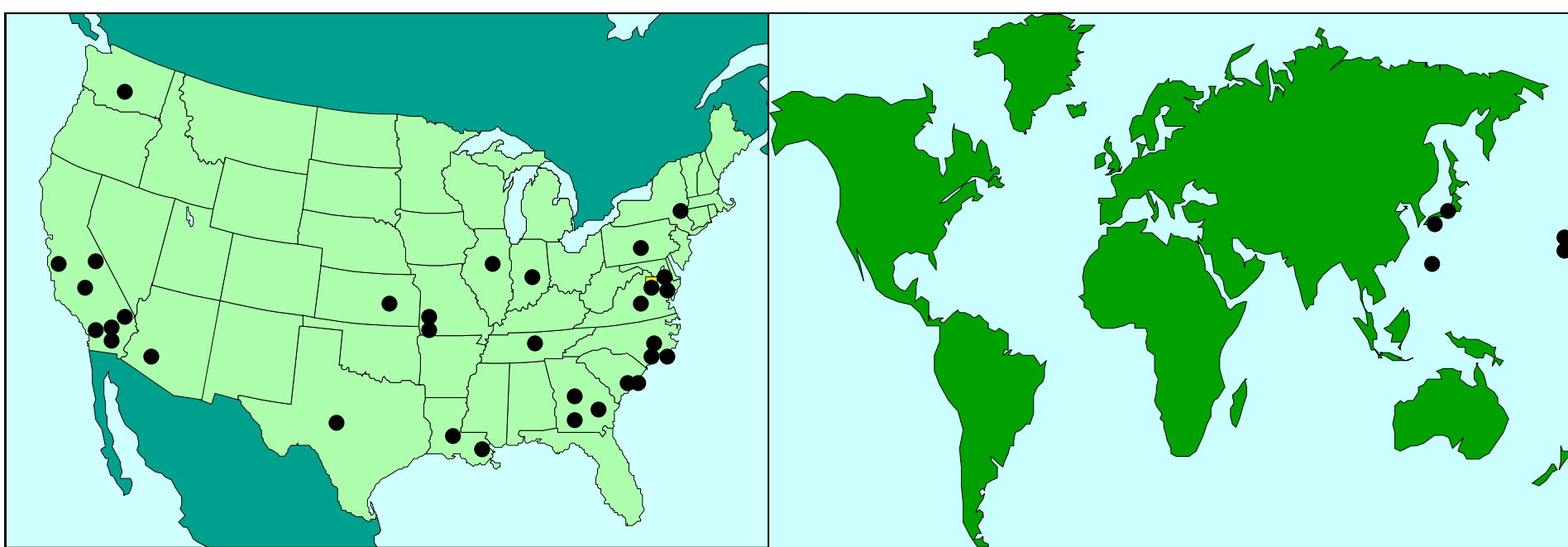
NMCI Approach

- Use Defense-in-Depth Strategy

- Map DITSCAP C&A activities into NMCI deployment strategy

- Meet DISN connection approval requirements

- Use NSA approved products for classified information protection

- Use DoD PKI

NMCI PKI Role

- Support MITNOC Call Center

- Configuration Management
  - Hardware
  - Plans, Procedures & SOPs

- RA Functions
  - Implement User Training
  - Directories
  - Request RRA/LRA Certificates
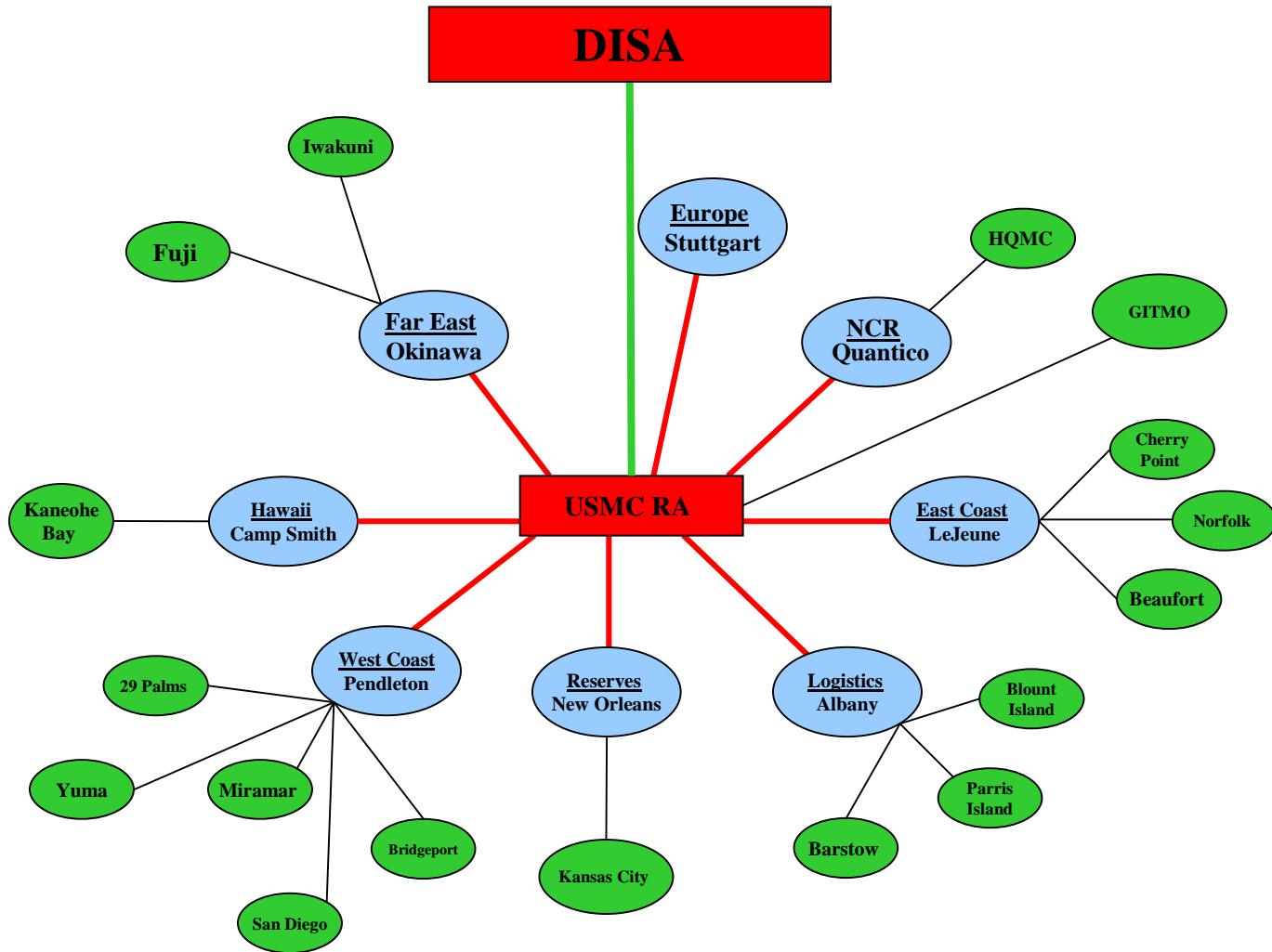
- Augment DEERS/RAPIDS VO/LRA

USMC DEERS/RAPIDS Locations

- 75 workstations @ 38 sites (active and reserve).

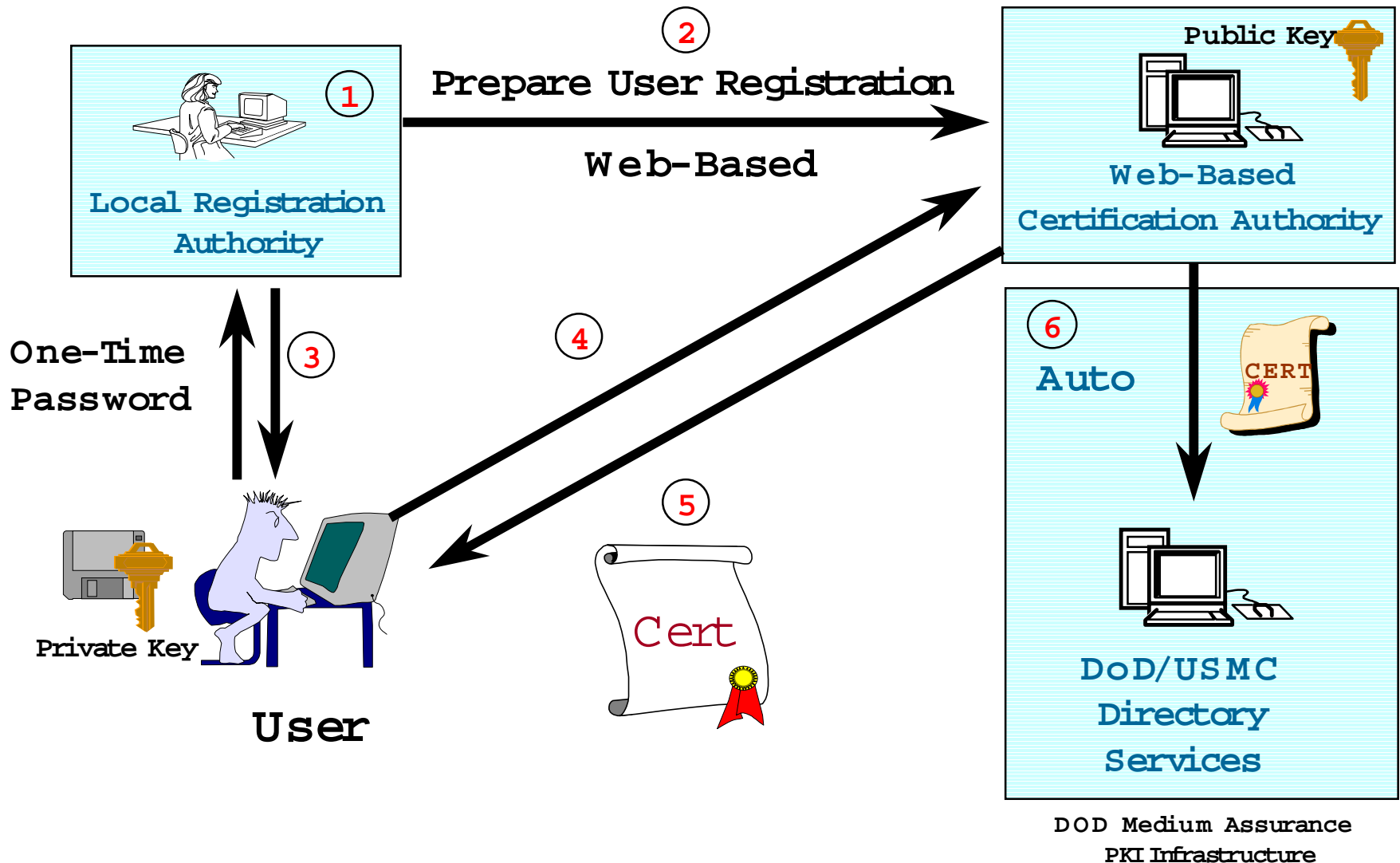- 15 additional workstations are planned as part of RAPIDS upgrades.

● DEERS/RAPIDS Locations

USMC RRA/LRA ARCHITECTURE

Registration Process

Local Registration Authority ①

② Prepare User Registration

Web-Based

Public Key

Web-Based Certification Authority

One-Time Password ③

④

⑤

Cert

Private Key

User

⑥ Auto

CERT

DoD/USMC Directory Services

DOD Medium Assurance PKI Infrastructure

Priorities

- Train RRA/LRAs
- Deploy Garrison Infrastructure
- Issuance of Class 3 S/W Certificates
- PKI Awareness/Education (End-users)
- Develop Tactical Infrastructure

Issues

- Limited CACs in use at NMCI AOR

- CAC/CAC Reader Compatibility

- PKI Migration Plan

Questions

LtCol T.T. Beck
Assistant Program Manager
CAC/SCT/PKI/PK-E
(703) 784-0870
Becktt@mcsc.usmc